

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

Your Affiant, Henry M. Cook, being duly sworn, hereby depose and state the following:

A. Introduction

1. Your Affiant is a Special Agent of the U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) (formerly the Department of Treasury, United States Customs Service, Office of Investigations). Your Affiant has been employed in this capacity since May 5, 2002. Your Affiant is currently assigned to the Resident Agent in Charge (RAC) office in Charleston, South Carolina, which is responsible for investigating violations of federal laws, including those relating to child pornography. As part of my employment with ICE, your Affiant received investigations training from the Federal Law Enforcement Training Center (FLETC) and in service training for violations relating to child pornography and investigations relating to computers. On December 13, 2006, your Affiant completed computer technician training and received CompTIA's A+ Certification. On March 1, 2007, your Affiant completed the Computer Investigative Specialist 2000 training curriculum in computer evidence recovery at the Federal Law Enforcement Training Center. As part of this course, your Affiant received training in the use of AccessData's Forensic Tool Kit (FTK), Guidance Software's Encase forensics software, and other software used in examining computers. On May 12, 2008, your Affiant completed Child Exploitation Investigations Training at the ICE Cyber Crimes Center and Training Academy. Your Affiant has personally investigated or been involved in over twenty investigations involving child pornography and has obtained multiple search warrants based on probable cause during the course of these investigations.

2. This affidavit is submitted in support of an application for a warrant to search for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway in Mountain View, California, that contains data relating to particular accounts associated with the electronic email addresses:

matissboy@gmail.com

which are further described in the following paragraphs and in Attachment A, as fully incorporated herein. As set forth herein, there is probable cause to believe that on the computer systems of Google., there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2251 (Production of Child Pornography) and Title 18, United States Code, Section 2252A(a) (Possession, Receipt, Distribution of Child Pornography).

B. Google

3. Based on my training and experience and investigation in this case, I have learned the following about Google:

a. Google, located at 1600 Amphitheatre Parkway in Mountain View, California, operates an email service known as "Gmail" through its web site at www.google.com, which is available free of charge to Internet users. Subscribers obtain an account by registering on the Internet with Google. Google asks subscribers to provide basic information such as name, zip code and other personal/biographical information; however, Google does not verify the information provided. Once Google email subscribers have completed their registration process, they may access their email accounts on servers maintained and/or owned by Google from any computer connected to the Internet located anywhere in the world;

b. Google maintains electronic records, including opened and unopened email pertaining to their subscribers, including account access information, email transaction information, and account application information;

c. Any email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Google. The message can remain on Google's servers indefinitely if the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically;

d. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually to the email provider of the email addressee. Google's users have the option of saving a copy of the email sent. If the sender does so, the email can remain on Google's system indefinitely. A sender can delete a previously sent and stored email message, thereby eliminating it from the sender's "Sent" box maintained at Google, but if the recipient of that same message is a Google email subscriber, the message will remain in the recipient's "Inbox" until the recipient deletes it or unless the recipient's account is subject to account size limitations;

e. A Google subscriber can store files, including emails and image files, on servers maintained and/or owned by Google; and

f. Google offer's its email subscribers the opportunity to access their accounts through a personalized or "home" web page, known as a "iGoogle" page. Subscribers can configure their "iGoogle" pages to display pre-set fields of information offered by Google or affiliated vendors. These fields of information include regional or specialized news headlines,

localized weather reports, specific team scores, select stock prices, airfares to select travel destinations, specific job listings, and maps.

C. Authority to Access Content of Electronic Communications

4. *Stored Communications.* If the government obtains a search warrant issued under the Federal Rules of Criminal Procedure, it can require a provider of email services to disclose the contents of a subscriber's stored email messages or other stored communications, without giving notice to that subscriber. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) of that Act enables law enforcement to seek a warrant requiring an Internet service provider to disclose the contents of electronic communications pursuant to the procedures in the Federal Rules of Criminal Procedure. Pursuant to Section 2703(g) of the Act specifies that a law enforcement agent need not be present to serve or execute the warrant.

a. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.

b. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) "electronic storage" means --

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

See Title 18, United States Code, Sections 2703(a), (b)

5. *Transactional (Non-Content) Data.* The government also has the authority to access non-content, transactional data that an Internet provider retains about its subscribers. Such transactional information might include the To: or From: lines on past email messages, the Internet Protocol ("IP") numbers used to route these messages over the Internet; log files showing dates, times, and methods of connecting to Google's computers; other Internet locations to/from which a subscriber came or went; purchases made; the number of visitors or "hits" a subscriber's web page has received, and services accessed through a subscriber's personalized ["home" or "iGoogle"] web pages. The government may access this transactional information with something less than a search warrant - namely a showing that there are "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." See 18

U.S.C. §§ 2703(d). Yet, the government also may access such non-content, transactional data using “a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . .” pursuant to Title 18, United States Code § 2703(c)(1)(A).

6. *Subscriber Information.* Pursuant to Title 18, United States Code § 2703(c)(2): the government may also obtain the following subscriber information from a service provider:

- a. name
- b. address
- c. local and long distance telephone connection records
- d. records of session times and durations;
- e. length of service (including start date) and types of service utilized;
- f. telephone or instrument number or other subscriber number or identity including any temporarily assigned network address such as an Internet Protocol Address;
- g. means and source of payment for such service (including any credit card or bank account number)

Under this statutory provision, the government may obtain such subscriber information using a subpoena, an “articulable facts” order, or a warrant as described above.

7. *The Authority of this Court.* A warrant for disclosure of the e-mail contents, transactional data, or subscriber records may be issued by any “court with jurisdiction over the offense under investigation,” see 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), and “a court of competent jurisdiction” includes --

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that --

- (i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title.

Title 18 U.S.C. § 2711(3). Thus, a search warrant may be issued by a federal magistrate in this district, even if the electronic records sought by the government reside in another district.

8. *Method of Service.* If this Court issues a warrant as requested by the government, a law enforcement officer need not be present to serve or execute that warrant upon Google. Pursuant to Title 18 U.S.C. § 2703(a):

The presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

Thus, a law enforcement officer may serve a warrant to an Internet provider by facsimile, and the Internet provider may return records to the officer via the mail or overnight courier. See also United States v. Bach, 310 F. 3d 1063 (8th Cir. 2002), *cert. denied*, 538 U.S. 993, 123 S.Ct. 1817 (2003).

D. Relevant Statutes

9. Title 18, United States Code, Section 2252A(a) (Possession, Receipt, Distribution of Child Pornography).

E. Definitions

10. The terms "minor", "sexually explicit conduct", "visual depiction", "producing", and "child pornography" are defined as set forth in Title 18 United States Code, Section 2256.

F. Probable Cause

11. On or about February 7, 2012, Gerald ROBERTS granted consent for HSI Charleston agents to assume is online identity known as jtease93@yahoo.com. ROBERTS is a known producer and trader of child pornography who pled guilty in U. S. District Court, Florence, SC on February 25, 2013, for producing child pornography in violation of Title 18, United States Code, Section 2251(a) and transporting child pornography in violation of Title 18, U.S.C. Section 2252A(a)(1). ROBERTS told your Affiant during an interview he set up the email account jtease93@yahoo.com for the purpose of trading child pornography

12. On or about February 24, 2013, an individual using the email address **matiboy@gmail.com** sent an email to the account jtease93@yahoo.com. Attached to the email is a file named FOLDER 79.rar. The attached file FOLDER 79.rar contains twenty-nine images with at least fifteen of the images involving prepubescent females engaged in sexually explicit activity including oral copulation and sexual intercourse with adult males.

13. On or about February 28, 2013, an HSI administrative summons was issued to Google for records related to email account **matiboy@gmail.com**. On March 6, 2013, Google provided the following information in response to the Summons;

GOOGLE SUBSCRIBER INFORMATION

Name: Tony Yayo

e-Mail: **matiboy@gmail.com**

Status: Enabled

Services: Emerald Sea Invite, Gmail, Google Drive, Google Mobile, Google Services,

Google Talk,

Knowledge Search, Picasa Web Albums, Transliteration, Web History

Secondary e-Mail: markerp@bk.ru

Created on: 2008/01/11-17:08:14-UTC

IP: 92.113.27.133, on 2008/01/11-17:08:14-UTC

Language Code: ru

SMS: 380665808723 [UA]

G. Conclusion

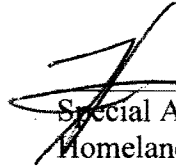
14. Based upon the facts set forth above, your affiant believes the user of the email account **matissboy@gmail.com** is involved in the distribution of child pornography and your affiant believes there is probable cause that on the computer systems owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway in Mountain View, California, there exists additional evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a) (Possession, Receipt, Distribution of Child Pornography). By this affidavit and application, I request that the Court issue a search warrant directed to Google, authorizing agents to search email and other information stored at Google and to seize the records and information, described in Attachment A, following the search procedure described in Attachment A, which is fully incorporated herein.

H. Delayed Notification

21. In accordance with 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I request that the warrant delay notification of the execution of the warrant for a period not to exceed 90 days because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation and result in adverse effects as defined

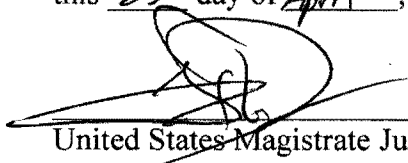
in Title 18, United States Code, Section 2705(a)(2), namely flight from prosecution, destruction of or tampering with evidence, and intimidation of potential witnesses.

Further your Affiant sayeth not.


Special Agent Henry M. Cook
Homeland Security Investigations

SUBSCRIBED and SWORN to before me

this 23 day of April, 2013.


United States Magistrate Judge